Übungen zur Algebraischen Zahlentheorie I

Wintersemester 2010/11

Universität Heidelberg
Mathematisches Institut
Prof. A. Schmidt
Dr. A. Holschbach

Blatt 13
Abgabetermin: Mittwoch, 02.02.2010, 16.15 Uhr

Aufgabe 1. Zeigen Sie: $3 \mid h_{\mathbb{Q}(\zeta_{23})}$.

Hinweis: Bestimmen Sie zunächst die Klassengruppe von $\mathbb{Q}(\sqrt{-23})$ und wenden Sie dann Korollar 5.31 an.

Aufgabe 2. Zeigen Sie: Zu jeder endlichen abelschen Gruppe A gibt es eine Galoiserweiterung $K|\mathbb{Q}$ mit $\mathrm{Gal}(K|\mathbb{Q}) \cong A$.

Hinweis: Schreiben Sie zunächst $A \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z}$ mit geeigneten $n_i \in \mathbb{N}$. Benutzen Sie dann Satz 6.11, um paarweise verschiedene Primzahlen $p_1, \ldots, p_r$ zu finden, so dass $p_i \equiv 1 \bmod n_i$ für alle i gilt. Folgern Sie, dass es in der Galoiserweiterung $\mathbb{Q}(\zeta_{p_1 \cdots p_r})|\mathbb{Q}$ einen Zwischenkörper K gibt, welcher die Behauptung erfüllt.

Aufgabe 3. Sei $K = \mathbb{Q}(\zeta)$ mit $\zeta = \zeta_5 = e^{2\pi i/5}$, und sei $\eta = \zeta + \zeta^{-1} \in \mathbb{Q}(\zeta)^+$.

(a) Zeigen Sie: Jede Einheit $\varepsilon \in E_K$ lässt sich (eindeutig) schreiben als $\varepsilon = \pm\zeta^l\eta^m$, $l \in \{0, \ldots, 4\}$, $m \in \mathbb{Z}$.

Hinweis: Zeigen Sie zunächst, dass $\eta = \frac{\sqrt{5}-1}{2}$, indem Sie nachweisen, dass es die eindeutige positive Nullstelle von $X^2 + X - 1$ ist. Verwenden Sie dann Satz 6.12 und Ihr Wissen über die Einheiten in $\mathbb{Q}(\sqrt{5})$.

(b) Beweisen Sie *Kummers Lemma* für $p = 5$: Sind $\varepsilon \in E_K, n \in \mathbb{Z}$ mit $\varepsilon \equiv n \bmod 5\mathbb{Z}[\zeta]$, so ist ε die fünfte Potenz einer Einheit $\varepsilon' \in E_K$.

Hinweis: Man schreibe $\varepsilon = \pm\zeta^l\eta^m$ wie in (a). Mit $\lambda = 1 - \zeta$ zeige man zunächst $\eta = 2 + \zeta^{-1}\lambda^2$ und folgere durch Betrachtung modulo (λ^2), dass $l = 0$. Anschließend betrachte man $\pm\eta^m$ modulo $(\lambda^4) = 5\mathbb{Z}[\zeta]$ und folgere $5|m$.

Aufgabe 4. Sei A ein Dedekindring. Zeigen Sie:

(a) Ist $0 \neq \mathfrak{p} \subset A$ ein Primideal, so ist $A_\mathfrak{p}$ ein Hauptidealring.

(b) Ein endlich erzeugter A-Modul M ist genau dann torsionsfrei, wenn er flach ist.

Hinweis: Benutzen Sie (a), die Sätze aus Abschnitt 7.2 und den Hauptsatz über endlich erzeugte Moduln über Hauptidealringen.

Zusatzaufgabe: Zum Abschluss wollen wir die Fermat'sche Vermutung für $p = 5$ beweisen: Die Gleichung

$$X^5 + Y^5 = Z^5 \tag{1}$$

hat keine ganzzahligen nichttrivialen Lösungen.

(a) Wie in der Vorlesung bereits erwähnt, ist der „erste Fall" einfach: Man betrachte die Restklassen von fünften Potenzen modulo 25 und folgere, dass es keine Lösung $(x, y, z) \in \mathbb{Z}^3$ von (1) mit $5 \nmid xyz$ geben kann.

(b) Daher können wir uns auf den „zweiten Fall" beschränken und ohne Einschränkung annehmen, dass $p \mid z$, also $z = p^r z_0$ für $r \in \mathbb{N}$, $p \nmid xyz_0$. Wir verwenden ab jetzt die Bezeichnungen aus Aufgabe 3 und folgern die Behauptung mit Hilfe von $p\mathbb{Z}[\zeta] = (\lambda^4)$ aus einer noch stärkeren Aussage:

Für $m \in \mathbb{N}$ gibt es keine $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta]$, $\lambda \nmid \alpha\beta\gamma$, mit

$$\prod_{i=0}^{4}(\alpha + \zeta^i\beta) = (\alpha^5 + \beta^5) = (\lambda^{5m}\gamma^5). \tag{2}$$

Im Folgenden nehme man an, es gebe eine Lösung α, β, γ, m von (2) mit minimalen m. Wir führen dies zu einem Widerspuch.

(c) Wegen $h_K = 1$ (Minkowski!) können wir ohne Einschränkung α, β, γ als paarweise teilerfremd annehmen. Zeigen Sie, dass $(\alpha + \zeta^i\beta, \alpha + \zeta^j\beta) = (\lambda)$ für beliebige $i \neq j$. Betrachten Sie die Differenzen der $\alpha + \zeta^i\beta$ modulo λ^2 und schließen Sie daraus, dass genau eines der $\alpha + \zeta^i\beta$ durch λ^2 teilbar ist. Folgern Sie, dass $m \geq 2$ und oBdA

$$\alpha + \beta = \varepsilon_0\lambda^{5m-4}\gamma_0^5, \qquad \alpha + \zeta^i\beta = \varepsilon_i\lambda\gamma_i^5 \quad \text{für } i = 1, \ldots, 4$$

mit $\varepsilon_i \in E_K, \gamma_i \in \mathbb{Z}[\zeta], \lambda \nmid \gamma_i$ für alle i.

(d) Zeigen Sie

$$\frac{\varepsilon_1}{\zeta\varepsilon_4}\gamma_1^5 + \gamma_4^5 = \frac{(1+\zeta)\varepsilon_0}{\zeta\varepsilon_4}\lambda^{5(m-1)}\gamma_0^5.$$

Benutzen Sie Lemma 6.16, um zu zeigen, dass es ein $n \in \mathbb{Z}$ gibt mit $\frac{\varepsilon_1}{\zeta\varepsilon_4} \equiv n \bmod 5\mathbb{Z}[\zeta]$. Folgern Sie mit Kummers Lemma aus Aufgabe 3, dass $\frac{\varepsilon_1}{\zeta\varepsilon_4} = \varepsilon^5$ für ein $\varepsilon \in E_K$. Aus der resultierenden Idealgleichung

$$\big((\varepsilon\gamma_1)^5 + \gamma_4^5\big) = (\lambda^{5(m-1)}\gamma_0^5)$$

lässt sich ein Widerspruch zur Minimalität von m ableiten.

Bemerkung: Obiger Beweis für den „zweiten Fall" lässt sich mit leichten Änderungen für jede reguläre Primzahl anwenden. Allerdings benötigt man dafür auch Kummers Lemma für beliebige reguläre Primzahlen, dessen allgemeiner Beweis entweder deutlich mehr Aufwand oder fortgeschrittenere Kenntnisse erfordert.